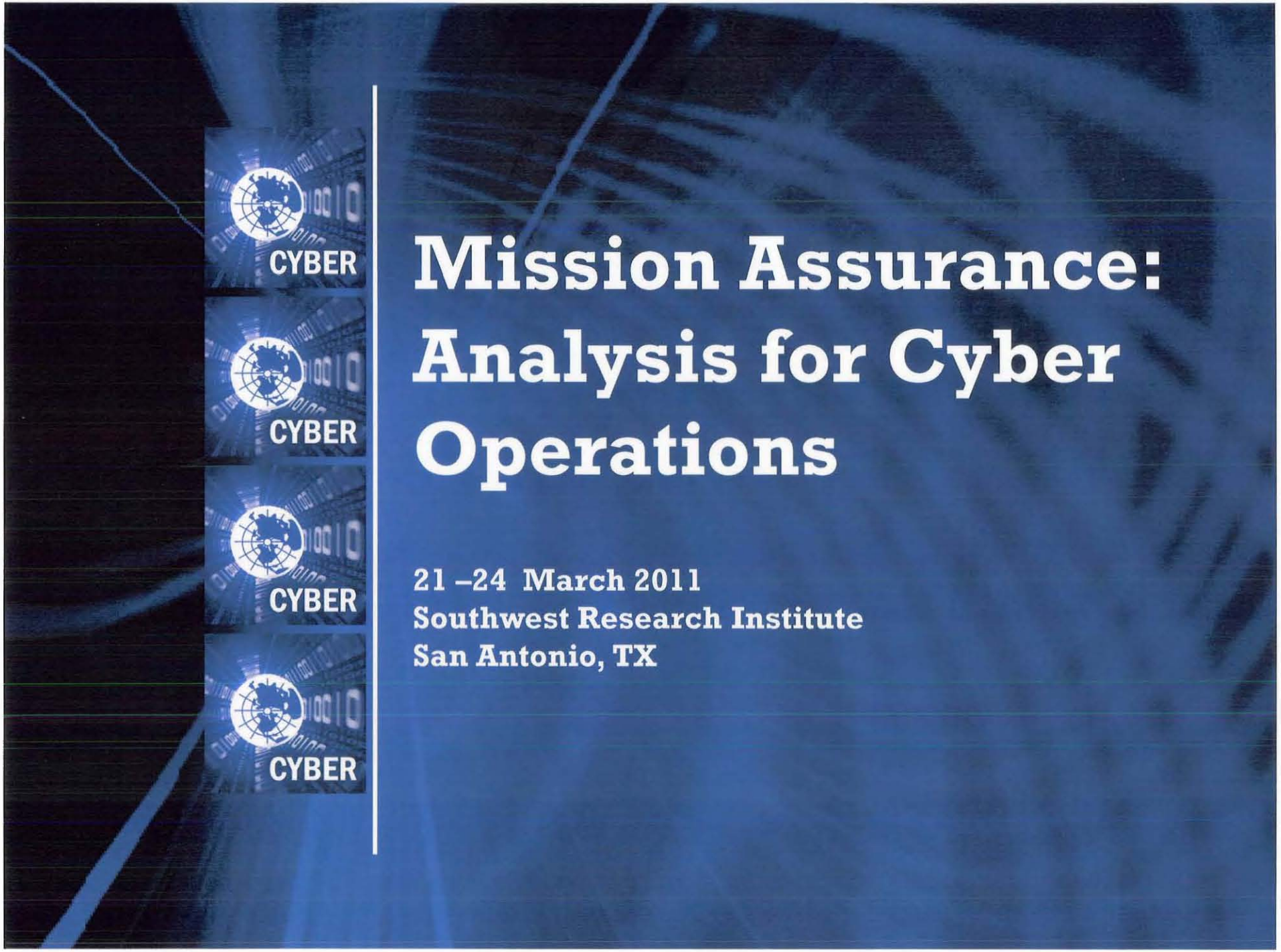

Mission Assurance: Analysis for Cyber Operations

21 –24 March 2011
Southwest Research Institute
San Antonio, TX

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
24 MAR 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Force Application	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **24th Air Force /ACCE,Lackland AFB,TX, 78243-713**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
MORS Mission Assurance: Analysis for Cyber Operations Special Meeting held in San Antonio, TX Mar 21-24, 2011.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**15**	

Working Group 4

Cyber Force Application

Chair – Col Robert Morris, 24 AF/ACCE
Co Chair, Mr Brian Williams, MITRE Corp

And on keyboard – Capt Geffert!

24 Mar 2011

WG 4 Acknowledgements

- Briefings:
  - *Computer Network Attack (CNA) Joint Munitions Effectiveness Manual (JMEM):* Dan Prettyman, HQ USSTRATCOM/J884
  - *Operational Assessment:* Major Mike HunsbergerUSCC/J375 Defensive Assessments Branch Chief
  - *LandWarNet NetOps Interoperability Study:* Peter Kerekanich, TRAC-FLVN

WG 4 Participants

- Mr. Frederick Bacon (719) 556-9826 frederick.bacon.ctr@peterson.af.mil, AFSPC/A9FC
- Mr. Stephen Bauer (703) 414-3146 stephen.a.bauer@saic.com SAIC
- CDR Scott Bunnay 703-413-1100 sbunnay@rand.org RAND Corporation
- Dr. Donald Duncan (443) 778-8912 donald.p.duncan@jhuapl.edu JHU/APL
- Mr. Pat Kotary 315 336-3306 kotaryp@ainfosec.com AIS, Inc.
- Dr. Barry McKinney 315 336 3306 mckinneyb@ainfosec.com Assured Information Security, Inc
- Kent Pickett 913-946-1905 kpickett@mitre.org The MITRE Corporation
- Mr. Daniel Prettyman 4022945815 prettymd@stratcom.mil USSTRATCOM
- Mr Jeff Ray, (402) 294-1208, rayj@stratcom.mil, USSTRATCOM/J812
- Dr. Stephen Torri (540) 653-1082, stephen.torri@navy.mil NSWC Dahlgren
- Ed Zarret 575-678-3508 ed.zarret@us.army.mil Army Research Laboratory
- Tim Autry, (210) 734-1728, tim_autry@sra.com, SRA International, Inc.
- Bill Sentlinger, (703)784-6044, bill.sentlinger@usmc.mil, MCCDC/OAD
- Bill Bernard, 703-697-0480, william.bernard@pentagon.af.mil, AF/CVR
- Peter Kerekanich, 913-684-9316, peter.kerekanich@us.army.mil, TRAC-FLVN
- Steve Walker, (540) 653-6096, swalker@jwac.mil, JWAC
- Torrys Johnson, (210) 925-2231, torrys.johnson@us.af.mil, 24 AF/A9L
- Capt Greg Jeong, (210) 395-1852, greg.jeong@us.af.mil, 24 AF/A9A
- Bill Bennett, 719-556-0942, william.bennett@peterson.af.mil, HQ AFSPC/A9F
- Dr. Akhil Shah, 310-393-0411, ashah@rand.org, RAND corp.
- Capt Sue St. Cyr, 210-395-9603, susanne.stcyr@us.af.mil, 624 OC/SRD
- Mr Brian Williams, 210-675-9640, bhwilliams@mitre.org, brian.williams.ctr@lackland.af.mil, MITRE Corp
- Capt Thomas Geffert, 210-395-7062, thomas.geffert@us.af.mil, 24 AF/A5

WG 4 Purpose/Focus:

Analytic requirements to enhance Operational Targeting and **increase relevance** for Cyber Operations in the Multi-Domain Battlefield. Specific areas will include a discussion of analysis to support determination of Militarily Relevant Cyber Targets, their contribution to the Combined Force Commander's objectives and **operational measures of performance and effectiveness**.

Key data questions…

1. Determine combat assessment needs for operational commanders.
2. Determine how Cyber operational effectiveness is measured wrt the CDRS objectives.
3. Determine "best of breed" methodologies for determining cyber MOE, MOP, MOO.
4. Investigate and normalize analytic methodologies that support combat assessment.
5. Recommend analytic tools and methodologies support combat assessment of Cyber Operations.

Key data questions…

1. Determine combat assessment needs for operational commanders.
2. How do we determine the operational impact of cyber operations wrt the CDRS objectives?

   - Operational effectiveness and impact are measured and assessed and represented in the same way as traditional military operations at the JTF/CC and above levels.
   - There are no differences in assessing the effects of cyber or other operations wrt CDR's objectives.

Key data questions…

3. What is the "best of breed" methodology for determining MOE. MOP, MOO for cyber Ops?

- Current Methodologies
  - TRAC (TRADOC Analysis) > issues to measures (I2M)
    - Targeting doctrine
    - JCIDS
      - JWAC - Modeling with a combination of tool metrics
    - NPS > Defend attack defend (DAD)
    - Exercises and Experiments
      - Review historical LL
    - Review CNO DB
    - Vignette based assessment

Key data questions…

4. Investigate and normalize analytic methodologies that support combat assessment.

- Incorporate Cyber effects **into current** models and analytic tools, exercises, wargames and experiments
  - Warfighter Conference (Staff member from 3, 5 and OR communities)
    - Tutorials (How you use the cyber tools)
  - "OR for Cyber" – Book/Manual

Key data questions…

5. Recommend analytic tools and methodologies support combat assessment of Cyber Operations.

- Follow Joint Targeting Doctrine
- Apply JCIDS to Cyber Acquisition
- Apply OR techniques to enhance exercises and experiments

WG 4 Gaps

- Data (availability and sharing) classification is not an excuse
- SysAd and Operator responses
- Behavioral modeling
- How we deal with unknowns intrusions and network behavior
- Understanding Network behavior resilience / predictive analysis (**Intel)
  - Mathematical understanding of effects from network changes (IONA)
- Weapons surrogate / data substitution for modeling what level of fidelity
- Adversary network uses / resilience/predictive analysis (** Intel)
- Avoid adversary detection / redirects / honey-pots (*TTP)
- Exercises / Experiments

WG 4 Findings

Tools required…..

1. OR model(s) that employ cyber weapons in combat environment to enable decision making….
2. Analysis of OPLANS compared to current and near term cyber capabilities
3. Engagement, Mission and Operational models and simulations
4. Campaign level analytic support via M&S
5. Cyber weapons effectiveness data
6. Weapons / target planning tool (NAWS?)
7. Web interface data repository (MIDB level data – CNO DB?)

Ways forward

1. Invite cyber HQE/Greybeards to review and guide normalization of cyber analytic efforts (attend MORSS….)
2. Incorporate OR methodologies across exercise planning and execution
3. Conduct "best use of Cyber forces" analyses and assessment
4. OPLAN vice capability roll up
5. Develop and Employ vignettes into War games/experiments
6. Bib/database of relevant cyber research and analytic tools (LL)

WG 4 Recommendations

- Incorporate cyber HQE/Greybeards into operations, exercises and analytic venues to help identify, promulgate and normalize analytic methodologies that support combat assessment (attend MORSS….)
- Introduce and Incorporate OR methodologies across exercise planning and execution
  - Formalize OR as part of the operational commander's staff as active participants, not only as "After Action" report writers
- Conduct "best use of Cyber forces" analyses and assessment
  - Command and Control Cost-benefit analysis of COTS vs GOTS
  - Optimize avenues of approach to adversary targets and effects
  - OPLAN vice capability roll up
- Develop and Employ vignettes into War games/experiments
- Publish a Bibliography/database of relevant cyber research and analytic tools (LL)
- A new Operations Research Manual for Cyber Operations

WG 4 Summary

- Operational Assessment at the JFC level is not affected by the introduction of cyber weapons and capabilities
  - i.e. cyber effects should be represented in the same way as kinetics
- Current analytic methods are applicable, but suffer from a lack of valid shared DATA to support substantive analyses
- Live fire test capability across "live" ranges and the "real world" are inadequate to support capability development and analyses
- Cyber M&S is evolving but is inadequate for effective effects assessment - who is the lead for cyber M&S?
- OR community must be involved at the beginning of all operations to adequately address combat assessment needs
- Today's questions are not unlike those posed and solved with Airpower, Space and IO… "How did OR assist their problems?"

Working Group 4

Cyber Force Application

Thank you, and good night!

24 Mar 2011